REMARKS

The Examiner has maintained the rejection of the claims under 35 U.S.C. 102(e) in view of the reference to Barlow et al. [U.S. Patent No. 6,038,551].

The amended Claim 1 now submitted for consideration has been restricted by specifying that the sender creates the transaction message "independently of any connection to a communications network and without computer dialogue with a receiver". This further delineates the central concept of the invention which is the elimination of any possibility that any second or third party or their computer will compromise the integrity of the transaction message at any time during the process of its being created and electronically signed and sealed by the sender. Support for this added wording to Claim 1 is to be found on page 5, lines 6-8 of the original description [PCT WO 98/52151].

Reference has been made to col. 14 of Barlow et al., the most nearly relevant passage being the description in col. 14, lines 42-58 of how a financial transaction is effected using a smart card and an automatic teller machine. Lines 48-52 read: "Next, the IC card and the banking application running on the ATM exchange authentication information. The banking application then conducts a financial transaction through the API to the IC card." It is submitted that this describes prior art methods where there is back-and-forth interaction between the sender and the receiver [the bank's computer] during the creation of the transaction method and prior to its being electronically signed by the sender. Typically, conducting a financial transaction through the API [Application Program Interface] to the IC card involves back and forth communication with a computer outside the sender's complete control. This is illustrated by the flow chart shown in Figs. 7-10 of Barlow et al. where steps 158-162, steps 170-174 and steps 180-186 all appear to involve back and forth interaction with a second

or third party computer **during** the creation of the signed transaction message. This is contrary to the concept of the invention as defined in the now amended main claim.

It is respectfully submitted that the narrowing amendment to Claim 1 now makes the present invention patentably distinct over the cited prior art.

Timothy Platt
Reg. No. 43,003

CLAIMS

1. (Currently amended) A method for performing electronic transactions, in which a sender of transaction messages is assigned a smart card with an associated unique identity and a private key stored in the card in a protected manner, and in which an associated public key is kept generally available, c h a r a c t e r i s e d in that in connection with an electronic transaction under the sender's own control, preferably through his own input of message information, the sender, independently of any connection to a communications network and without computer dialogue with a receiver, creates a transaction message, which contains information necessary for the transaction, and, in his smart card, provides the created transaction message with his digital signature while using his own private key for subsequent output and transmission of the transaction message.

2. (Original) A method as claimed in claim 1, c h a r a c t e r i s e d in that the transaction message contains information on sender, receiver, amount and preferably a transaction serial number.

3. (Previously amended) A method as claimed in claim 1 c h a r c a c t e r i s e d in that the transaction message is created off-line, i.e. not connected to the communications network that is used for the subsequent transmission of the transaction message.

4. (Original) A method as claimed in claim 3, c h a r a c t e r i s e d in that the transaction message is created off-line.

5. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the transaction message is created in the smart card.

6. (Previously amended) A method as claimed in claim 5, c h a r a c t e r i s e d in that the transaction message is created

with the aid of software inserted in the smart card in advance and preferably also sender information inserted in the card in advance.

7. (Previously amended) A method as claimed in claim 5, c h a r a c t e r i s e d in that information required for the transaction message is input with the aid of input means arranged on the smart card, the card preferably being a so-called advanced smart card.

8. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that information necessary for the transaction message is input with the aid of a protected card terminal.

9. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that information necessary for the transaction message is input with the aid of a separate card communication unit, the latter preferably also being a card activator.

10. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that information necessary for the transaction message is input with the aid of a telecommunications unit controlled by the smart card, especially a mobile telecommunications unit such as a mobile phone.

11. (Previously amended) A method as claimed in claim 1,c h a r a c t e r i s e d in that the transaction message contains sender information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

12. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the transaction message contains receiver information in the form of at least one of the following pieces of information: a card number, a cash card number, a

charge card number, a credit card number, an account number, an invoice number and an ID number.

13. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is sent to a card or account administrator regarding the sender or receiver, that the digital signature of the transaction message is authenticated by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that in case of authenticity, the receiver is credited with the transaction amount by a clearing process.

14. (Original) A method as claimed in claim 13, c h a r a c t e r i s e d in that the signed transaction message is first sent to the receiver, who optionally after his own checking of the digital signature of the message forwards the signed transaction message to said card or account administrator.

15. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is encrypted by using a public key belonging to the addressee, to whom the transaction message is sent, that the encrypted, signed transaction message is sent to the addressee, that the addressee by using his private key decrypts the signed transaction message, that the digital signature of the transaction message is authenticated by using the public key which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

16. (Original) A method as claimed in claim 15, c h a r a c t e r i s e d in that the addressee is the receiver, that the receiver, after decryption, sends the signed transaction message to a card or account administrator, whereupon said authentication takes place.

17. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is encrypted by using the sender's public key and is provided with sender information and is then sent to a card or account administrator, who has the sender's private key and who preferably has issued the user's smart card, that said administrator decrypts the received encrypted message by using said private key, that authentication of the digital signature of the decrypted transaction message takes place by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

18. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d in that the signed transaction message is sent non-encrypted, especially via a public communications network, such as the Internet or a telecommunications network.

19. (Previously amended) A method as claimed in claim 1, c h a r a c t e r i s e d, in that the signed transaction message is sent by e-mail.

20.(Original) A method as claimed in any one of claims 1-18, c h a r a c t e r i s e d in that the signed transaction message is sent via a mobile telephone network, especially by using a so-called SMS service.

21.(Original) A smart card for carrying out electronic transactions, comprising means for storing card identification information, means for protected storing of a private key, means for storing an asymmetrical algorithm, means for input of transaction information into the card, processor means for creating in the card a transaction message based on input transaction information, such as information on amount and receiver, and optionally information stored in the card, such as information on sender and preferably a serial number, and for provid-

ing the transaction message with a digital signature on the basis of said private key and said asymmetrical algorithm, and means for output of the signed transaction message.

22. (Previously amended) A card as claimed in claim 21, c h a r a c t e r i s e d in that the card is of a so-called advanced type.

23. (Original) A combination of a smart card and a user-controlled communication unit, which is arranged for communication with the smart card and with which the card is adapted to be combined with a view to producing an electronic transaction message, the card comprising means for protected storing of a private key, means for storing an asymmetrical algorithm and processor means for providing a created transaction message with a digital signature based on said private key and said algorithm, and said communication unit comprising means for input of transaction information, and means being arranged in the communication unit and/or in the card for creating said transaction message.

24. (Original) A combination as claimed in claim 23, c h a r a c t e r i s e d in that the communication unit is a mobile telecommunication device.

25. (Original) A combination as claimed in claim 23, c h a r a c t e r i s e d in that the communication unit is a combined card activator and information inputter/processor.

26. (Original) Use of a smart card with a private key stored therein for providing, independently of the communications network, an electronic transaction message provided with a digital signature based on the private key.

27. (Previously added) A method as claimed in claim 2, c h a r a c t e r i s e d in that the transaction message is created offline, i.e. not connected to the communications network that is issued for the subsequent transmission of the transaction message.

28. (Previously added) A method as claimed in claim 6, c h a r a c t e r i s e d in that information required for the transaction message is input with the aid of input means arranged on the smart card, the card preferably being a so-called advanced smart card.

29. (Previously added) A method as claimed in claim 27, c h a r a c t e r i s e d in that the transaction message is created off-line.